Team: Human Error Is A Myth

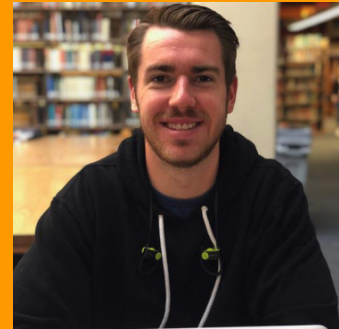
Graham Foster
(Lead)

Fernando Mendoza
(scribe)

Omer Cohen

Diego Segundo

Quintin Hill

Blake Johnson

Problem:

- Cyber Security analysts and pen testing teams have to manually search through a multitude of websites and forums on both the web and darkweb for relevant information
- Time Consuming
- Lacks Automation and Centralization

Our Solution

- Centralized and Automated
- Web Application
  - Central Console
  - Simultaneously scrapes: paste sites, pwned database, darkweb marketplaces
- Reduce Noise with granular filters like: email address, usernames, wallet ID's, credit cards, keywords, etc…
- Analysis Algorithm
- Proactive Alerting System

Use Cases

- **Offensive**
  - Pen Testing Teams
    - Save time and find valuable information that can lead to an exploit

- **Defensive**
  - Security Analysts
  - E.g. Bank of America Security Analyst

Modules

- **HaveIBeenPwned**
  - Searches for email and password exposure
  - Uses api and returns JSON object of the data.
- **Pastebin**
  - Searches for keywords
  - Uses web scraping and pastebin api to return JSON object of the data.
- **DarkWeb**
  - Searches for keywords
  - Uses web scraping to search darknet marketplaces, and paste sites for leaks.

Demo

Technologies Employed

Docker

- Docker packages our code and its dependencies into a lightweight executable package

- Ensures that the project is consistent for the whole team, so that we do not have to worry about dependency issues.
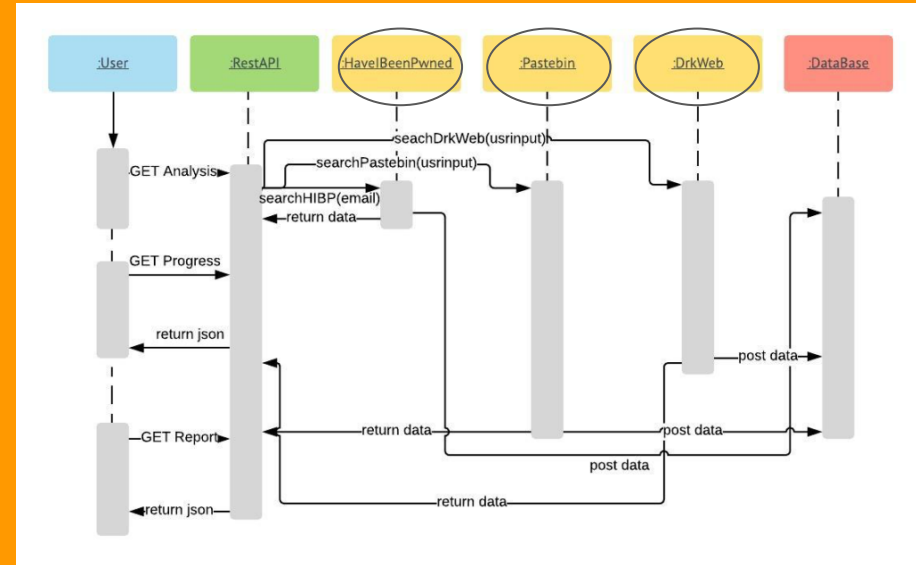
Selenium Scraping

- Used in conjunction with Pastebin's scraping api to search for keywords in Pastebin's infrastructure.

- Primary tool for DarkWeb module using Tor browser driver.

Asynchronous Microservices

- ● Separate microservices for each module
  - ○ Allows for independence between modules
  - ○ Developers can call select microservices
  - ○ Parallel searching

RESTful API

- Pre-defined, standardized and stateless endpoints allow for ease of integration
- Allows for third party integrations

HTTP METHOD	GET
CRUD OP	READ
/analyze/Quintin-Hill	List results on all
/analyze/hibpwned/quill1316@yahoo.com	Results from hibpwned
/analyze/pastebin/quintinhill	Results from pastebin
/analyze/DrkWeb/Quintin Hill	Results from darkweb

Next Steps

- Back end
    - Polish up the backend Implementation Testing
    - Complete Analysis Algorithm
- Front end
    - Parse the json objects
    - Improve the UI
    - Improve testing
- Feature Enhancements: Scheduled Scanning, Alerting